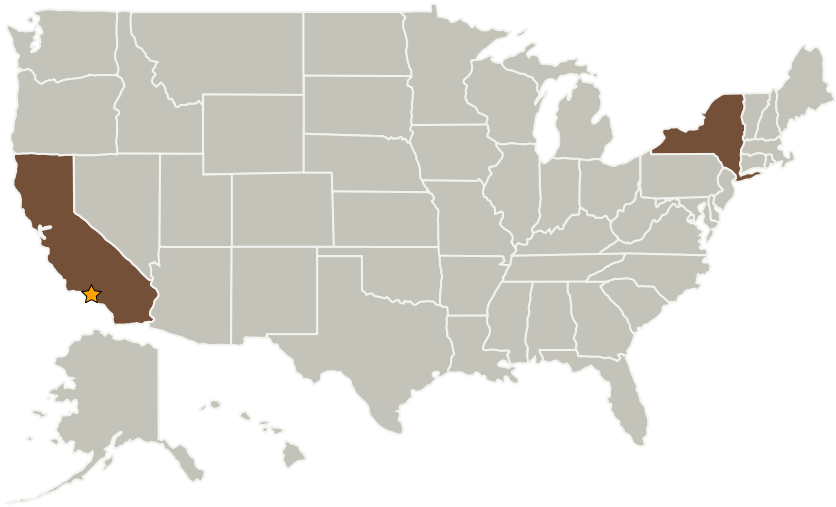
Static Detection of Bugs in Embedded Software Using Lightweight Verification, Phase II

Completed Technology Project (2007 - 2009)

Project Introduction

Validating software is a critical step in developing high confidence systems. Typical software development practices are not acceptable in systems where failure leads to loss of life or other high costs. Software best practices for high confidence systems are often codified as coding rules. Adhering to these practices can increase software readability and predictability, thereby enhancing quality. However, adherence is limited by the lack of high-quality tools to measure adherence automatically. Checking rule conformance requires a diverse set of software analysis technologies, ranging from syntactic analysis to sophisticated inference of runtime behavior. By combining lightweight verification techniques with other scalable analysis techniques that target syntactic and other static properties, we will create a tool that flags violations for almost all the rules typically applied to high-assurance code. Our Phase I work demonstrated the feasibility of this approach. In Phase I, we developed a tool for checking compliance with rules developed for JPL flight software. The tool leveraged GrammaTech's existing technology for static analysis, including facilities for analyzing a program's abstract syntax tree, control-flow graph, and inferred runtime behavior. The prototype successfully checks a set of rules designed for high-assurance software. Our experiments show that the tool adds only minimal overhead to our CodeSonar bug-finding tool, and generates few or no spurious results that could distract or annoy users.

Primary U.S. Work Locations and Key Partners



Static Detection of Bugs in Embedded Software Using Lightweight Verification, Phase II

Table of Contents

Organizational Responsibility

Responsible Mission Directorate:

Space Technology Mission Directorate (STMD)

Lead Center / Facility:

Jet Propulsion Laboratory (JPL)

Responsible Program:

Small Business Innovation Research/Small Business Tech Transfer

Static Detection of Bugs in Embedded Software Using Lightweight Verification, Phase II

Completed Technology Project (2007 - 2009)

Organizations Performing Work	Role	Type	Location
★Jet Propulsion Laboratory(JPL)	Lead Organization	NASA Center	Pasadena, California
GrammaTech, Inc.	Supporting Organization	Industry	Ithaca, New York

Primary U.S. Work Locations	
California	New York

Project Management

Program Director:

Jason L Kessler

Program Manager:

Carlos Torrez

Technology Areas

Primary:

- TX11 Software, Modeling, Simulation, and Information Processing
  - TX11.1 Software Development, Engineering, and Integrity
    - TX11.1.2 Verification and Validation of Software systems